Uniform distribution of linear recurrence sequences in residue class systems

Tamás Herendi

Random number sequences play an important role in numerical computations. In general, uniformly distributed sequences are the most useful in different applications. It is well known that linear recurrence sequences can be used for generating pseudorandom number sequences.

Let R be a Dedekind-domain, u be a linear rekurrence sequence and let P be a prime ideal in R. The sequence u is periodic, if we reduce modulo an arbitrary ideal I of R. We will say that u is uniformly distributed modulo I, if every residue class appear with the same frequency in a full period of u modulo I.

Several result deal with the conditions on parameters of linear recurring sequences which are uniformly distributed.

Our main result gives a possibility to determine linear recurrence sequences with arbitrarily big period length in arbitrarily big residue systems. The last property is important if we want to transform our sequence into the $[0,1]$ interval. The bigger the residue system is the smoother the transformed sequence.

The precise formulation of the result is the following:

Theorem 1 *Let $P \in R$ be a prime ideal with $\pi \in \mathbb{Z}$ prime norm, $d \geq 2$ an integer, u a dth order linear recurring sequence in R and $S = \frac{3d^2+9d}{2} + 1$. If u is uniformly distributed $(\mathrm{mod}\ P)^S$ then also uniformly distributed $(\mathrm{mod}\ P)^s$ for any $s \in \mathbb{N}$.*